

There is exactly one $\mathbb{Z}_2\mathbb{Z}_4$ -cyclic 1-perfect code

Joaquim Borges and Cristina Fernández-Córdoba

Abstract

Let \mathcal{C} be a $\mathbb{Z}_2\mathbb{Z}_4$ -additive code of length $n > 3$. We prove that if the binary Gray image of \mathcal{C} , $C = \Phi(\mathcal{C})$, is a 1-perfect nonlinear code, then \mathcal{C} cannot be a $\mathbb{Z}_2\mathbb{Z}_4$ -cyclic code except for one case of length $n = 15$. Moreover, we give a parity check matrix for this cyclic code. Adding an even parity check coordinate to a $\mathbb{Z}_2\mathbb{Z}_4$ -additive 1-perfect code gives an extended 1-perfect code. We also prove that any such code cannot be $\mathbb{Z}_2\mathbb{Z}_4$ -cyclic.

Index Terms

Perfect codes, $\mathbb{Z}_2\mathbb{Z}_4$ -additive cyclic codes, simplex codes.

I. INTRODUCTION

A $\mathbb{Z}_2\mathbb{Z}_4$ -linear code C is the binary Gray image of a $\mathbb{Z}_2\mathbb{Z}_4$ -additive code $\mathcal{C} \subseteq \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, and if $\beta = 0$, then C is a binary linear code. If $\alpha = 0$, then C is called \mathbb{Z}_4 -linear. In 1997, a first family of $\mathbb{Z}_2\mathbb{Z}_4$ -linear 1-perfect codes was presented in [11] in the more general context of translation-invariant propelinear codes. Lately, in 1999, all $\mathbb{Z}_2\mathbb{Z}_4$ -linear 1-perfect codes were fully classified in [6]. Specifically, for every appropriate values of α and β , there exists exactly one $\mathbb{Z}_2\mathbb{Z}_4$ -linear 1-perfect code C . Note that when $\beta = 0$, then C is a Hamming code. In subsequent papers ([5] and [9]), $\mathbb{Z}_2\mathbb{Z}_4$ -linear extended 1-perfect codes were also classified. But it was not until 2010, when an exhaustive description of general $\mathbb{Z}_2\mathbb{Z}_4$ -linear codes appeared [3]. More recently, in 2014, $\mathbb{Z}_2\mathbb{Z}_4$ -cyclic codes have been defined in [1], and also studied in [4].

After all these papers, a natural question is to ask for the existence or nonexistence of $\mathbb{Z}_2\mathbb{Z}_4$ -cyclic 1-perfect codes, of course, excluding the linear (Hamming) case when $\beta = 0$. In this paper, we show that such codes do not exist with only one exception. This unique $\mathbb{Z}_2\mathbb{Z}_4$ -cyclic 1-perfect code has binary length 15, with $\alpha = 3$ and $\beta = 6$. We also give a parity check matrix for such code. If we add an even parity check coordinate to a $\mathbb{Z}_2\mathbb{Z}_4$ -linear 1-perfect code, then we obtain a $\mathbb{Z}_2\mathbb{Z}_4$ -linear extended 1-perfect code. We show that none of these codes can be $\mathbb{Z}_2\mathbb{Z}_4$ -cyclic.

Manuscript received Month day, year; revised Month day, year.

J. Borges is with the Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, 08193-Bellaterra, Spain (e-mail: joaquim.borges@uab.cat)

C. Fernández-Córdoba is with the Department of Information and Communications Engineering, Universitat Autònoma de Barcelona, 08193-Bellaterra, Spain (e-mail: cristina.fernandez@uab.cat).

This work has been partially supported by the Spanish MICINN grant TIN2013-40524-P and by the Catalan AGAUR grant 2014SGR-691.

The paper is organized as follows. In the next section, we give basic definitions and properties. Moreover, we give the type of all $\mathbb{Z}_2\mathbb{Z}_4$ -linear 1-perfect codes, computing some parameters that were not specified in [6]. In Section III, we give the main results of this paper. First, we prove that in a $\mathbb{Z}_2\mathbb{Z}_4$ -cyclic 1-perfect code, β must be a multiple of α . This, immediately excludes a lot of cases. For the remaining ones, using a key property of simplex codes, we prove that α cannot be greater than 3. Therefore, finally, we have only one possible case when $\alpha = 3$ and $\beta = 6$. In Example 3.2, we give a parity check matrix for this code in a cyclic form. In Section IV, we prove that a $\mathbb{Z}_2\mathbb{Z}_4$ -linear extended 1-perfect code, with $\alpha > 0$, cannot be $\mathbb{Z}_2\mathbb{Z}_4$ -cyclic.

II. PRELIMINARIES

Denote by \mathbb{Z}_2 and \mathbb{Z}_4 the rings of integers modulo 2 and modulo 4, respectively. A binary code of length n is any non-empty subset C of \mathbb{Z}_2^n . If that subset is a vector space then we say that it is a linear code. Any non-empty subset C of \mathbb{Z}_4^n is a quaternary code of length n , and an additive subgroup of \mathbb{Z}_4^n is called a quaternary linear code. The elements of a code are usually called codewords.

Given two binary vectors $u, v \in \mathbb{Z}_2^n$, the (Hamming) distance between x and y , denoted $d(u, v)$, is the number of coordinates in which they differ. The (Hamming) weight of any vector $z \in \mathbb{Z}_2^n$, $w(z)$, is the number of nonzero coordinates of z . The Lee weights of $0, 1, 2, 3 \in \mathbb{Z}_4$ are $0, 1, 2, 1$ respectively, and the Lee weight of $a \in \mathbb{Z}_4^m$, $w_L(a)$, is the rational sum of the Lee weights of its components. If $a, b \in \mathbb{Z}_4^m$, then the Lee distance between a and b is $d_L(a, b) = w_L(a - b)$. For a vector $\mathbf{u} \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ we write $\mathbf{u} = (u \mid u')$ where $u \in \mathbb{Z}_2^\alpha$ and $u' \in \mathbb{Z}_4^\beta$. The weight of \mathbf{u} is $w(\mathbf{u}) = w(u) + w_L(u')$. If $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, the distance between $\mathbf{u} = (u \mid u')$ and $\mathbf{v} = (v \mid v')$ is defined as $d(\mathbf{u}, \mathbf{v}) = d(u, v) + d_L(u', v')$. The classical Gray map $\phi: \mathbb{Z}_4 \rightarrow \mathbb{Z}_2^2$ is defined by

$$\phi(0) = (0, 0), \quad \phi(1) = (0, 1), \quad \phi(2) = (1, 1), \quad \phi(3) = (1, 0).$$

If $a = (a_1, \dots, a_m) \in \mathbb{Z}_4^m$, then the Gray map of a is the coordinatewise extended map $\phi(a) = (\phi(a_1), \dots, \phi(a_m))$. We naturally extend the Gray map for vectors $\mathbf{u} = (u \mid u') \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ so that $\Phi(\mathbf{u}) = (u \mid \phi(u'))$. Clearly, the Gray map transforms Lee distances and weights to Hamming distances and weights. Hence, if $\mathbf{u}, \mathbf{v} \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, we have that $d(\mathbf{u}, \mathbf{v}) = d(\Phi(\mathbf{u}), \Phi(\mathbf{v}))$.

A binary code C of length n is called 1-perfect if any vector not in C is at distance one from exactly one codeword in C . Such codes have minimum distance 3 between any pair of codewords, and the cardinality is $|C| = 2^n/(n+1)$. It is well known that $n = 2^t - 1$, for some $t \geq 2$ and hence $|C| = 2^{2^t-t-1}$. For any t , there is exactly one linear 1-perfect code, up to coordinate permutation, which is called the Hamming code. An extended 1-perfect code C' is obtained by adding an even parity check coordinate to a 1-perfect code C . In this case, C' has minimum distance 4, length $n + 1 = 2^t$, and size $|C'| = 2^{2^t-t-1}$.

The dual of a binary Hamming code is a constant weight code called *simplex*. The dual of an extended Hamming code is a linear *Hadamard* code. In this paper, we make use of two important properties [8], [10]:

- (a) A binary Hamming code is cyclic, that is, its coordinates can be arranged such that the cyclic shift of any codeword is again a codeword. Therefore, simplex codes are also cyclic.

- (b) An extended Hamming code of length greater than 4 is not cyclic. Hence, a linear Hadamard code of length greater than 4 is not cyclic.

A $\mathbb{Z}_2\mathbb{Z}_4$ -additive code \mathcal{C} is an additive subgroup of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$. Such codes are extensively studied in [3]. Since \mathcal{C} is a subgroup of $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, it is also isomorphic to a group $\mathbb{Z}_2^\gamma \times \mathbb{Z}_4^\delta$. Therefore, \mathcal{C} is of type $2^\gamma 4^\delta$ as a group, it has $|\mathcal{C}| = 2^{\gamma+2\delta}$ codewords, and the number of codewords of order less than two in \mathcal{C} is $2^{\gamma+\delta}$.

Let X (respectively Y) be the set of \mathbb{Z}_2 (respectively \mathbb{Z}_4) coordinate positions, so $|X| = \alpha$ and $|Y| = \beta$. Unless otherwise stated, the set X corresponds to the first α coordinates and Y corresponds to the last β coordinates. Call \mathcal{C}_X (respectively \mathcal{C}_Y) the punctured code of \mathcal{C} by deleting the coordinates outside X (respectively Y), and removing repeated codewords, if necessary. Let \mathcal{C}_b be the subcode of \mathcal{C} which contains all order two codewords and the zero codeword. Let κ be the dimension of $(\mathcal{C}_b)_X$, which is a binary linear code.

According to [3], and considering all these parameters, we say that \mathcal{C} is a $\mathbb{Z}_2\mathbb{Z}_4$ -additive code of type $(\alpha, \beta; \gamma, \delta; \kappa)$. The binary Gray image of \mathcal{C} is $C = \Phi(\mathcal{C}) = \{\Phi(\mathbf{x}) \mid \mathbf{x} \in \mathcal{C}\}$. In this case, C is called a $\mathbb{Z}_2\mathbb{Z}_4$ -linear code of type $(\alpha, \beta; \gamma, \delta; \kappa)$ and its length is $n = \alpha + 2\beta$.

The standard inner product in $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$, defined in [3], can be written as

$$\mathbf{u} \cdot \mathbf{v} = 2 \left(\sum_{i=1}^{\alpha} u_i v_i \right) + \sum_{j=1}^{\beta} u'_j v'_j \in \mathbb{Z}_4,$$

where the computations are made taking the zeros and ones in the α binary coordinates as quaternary zeros and ones, respectively. The dual code of \mathcal{C} , is defined in the standard way by

$$\mathcal{C}^\perp = \{\mathbf{v} \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta \mid \mathbf{u} \cdot \mathbf{v} = 0, \text{ for all } \mathbf{u} \in \mathcal{C}\}.$$

The types of dual codes are related in [3].

Proposition 2.1 ([3]): If \mathcal{C} is a $\mathbb{Z}_2\mathbb{Z}_4$ -additive code of type $(\alpha, \beta; \gamma, \delta; \kappa)$, then its dual code \mathcal{C}^\perp is of type

$$(\alpha, \beta; \alpha + \gamma - 2\kappa, \beta - \gamma - \delta + \kappa; \alpha - \kappa).$$

Let C be a $\mathbb{Z}_2\mathbb{Z}_4$ -linear 1-perfect code. Then, the corresponding $\mathbb{Z}_2\mathbb{Z}_4$ -additive code $\Phi^{-1}(C)$ is also called 1-perfect code. Such codes are completely characterized.

Proposition 2.2 ([6]):

- (i) Let $n = 2^t - 1$, where $t \geq 4$. Then, for every r such that $2 \leq r \leq t \leq 2r$, there is exactly one $\mathbb{Z}_2\mathbb{Z}_4$ -linear 1-perfect code of length n , up to coordinate permutation, with parameters $\alpha = 2^r - 1$ and $\beta = 2^{t-1} - 2^{r-1}$.
- (ii) There are no other $\mathbb{Z}_2\mathbb{Z}_4$ -linear 1-perfect codes.

Here, we strength a little this result by computing the type of these codes. Since r and t completely determine a $\mathbb{Z}_2\mathbb{Z}_4$ -linear 1-perfect code, we denote such code by $C_{r,t}$. The corresponding $\mathbb{Z}_2\mathbb{Z}_4$ -additive code is $\mathcal{C}_{r,t} = \Phi^{-1}(C_{r,t})$.

Proposition 2.3: Let $\mathcal{C}_{r,t}$ be of type $(\alpha, \beta; \gamma, \delta; \kappa)$ and let $(\mathcal{C}_{r,t})^\perp$ be the dual code of type $(\bar{\alpha}, \bar{\beta}; \bar{\gamma}, \bar{\delta}; \bar{\kappa})$. Then,

(i) The parameters of $\mathcal{C}_{r,t}$ are:

$$\begin{aligned}\alpha &= 2^r - 1; \quad \beta = 2^{t-1} - 2^{r-1}; \\ \gamma &= 2^r - 1 - 2r + t; \\ \delta &= 2^{t-1} - 2^{r-1} + r - t; \\ \kappa &= \gamma.\end{aligned}$$

(ii) The parameters of $(\mathcal{C}_{r,t})^\perp$ are:

$$\begin{aligned}\bar{\alpha} &= \alpha; \quad \bar{\beta} = \beta; \\ \bar{\gamma} &= 2r - t; \quad \bar{\delta} = t - r; \\ \bar{\kappa} &= \bar{\gamma}.\end{aligned}$$

Proof: The parameters α , β , $\bar{\alpha}$ and $\bar{\beta}$ follow directly from Proposition 2.2.

On the one hand, the binary linear code $C_0 = \{(x \mid 0, \dots, 0) \in \mathcal{C}_{r,t}\}_X$ is clearly 1-perfect, i.e. a Hamming code. Hence, C_0 has dimension $2^r - r - 1$. This means that the zero codeword in $(\mathcal{C}_{r,t})_Y$ (and any other one) is repeated 2^{2^r-r-1} times in $\mathcal{C}_{r,t}$. On the other hand, consider a vector of the form

$$\mathbf{u} = (u \mid u') = (0, \dots, 0 \mid 0, \dots, 0, 2, 0, \dots, 0) \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta,$$

where $\alpha = 2^r - 1$ and $\beta = 2^{t-1} - 2^{r-1}$. Since the minimum distance in $\mathcal{C}_{r,t}$ is 3, the minimum weight is also 3 because $\mathcal{C}_{r,t}$ is distance invariant [11]. Hence \mathbf{u} must be at distance one from a weight 3 codeword $\mathbf{x} = (x \mid x')$, where $w(x) = 1$ and $x' = u'$. Indeed, if $w(x) = 0$ and $w(x') = 3$, then $2\mathbf{x}$ would have weight 2. Therefore, $(\mathcal{C}_{r,t})_Y$ has 2^β distinct codewords of order two (including here the zero codeword). We conclude that $\mathcal{C}_{r,t}$ has $2^\beta \cdot 2^{2^r-r-1}$ order two codewords (again, including the zero codeword). Thus, the dimension of $(\mathcal{C}_{r,t})_b$ is

$$\gamma + \delta = \beta + 2^r - r - 1 = 2^{t-1} + 2^{r-1} - r - 1. \quad (1)$$

The size of $\mathcal{C}_{r,t}$ is 2^{2^t-t-1} . Therefore,

$$\gamma + 2\delta = 2^t - t - 1. \quad (2)$$

Combining Equations 1 and 2, we obtain the values of γ and δ .

As can be seen in [6], the quotient group $\mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta / \mathcal{C}_{r,t}$ is isomorphic to $\mathbb{Z}_2^{2^r-t} \times \mathbb{Z}_4^{t-r}$. In other words, $\mathcal{C}_{r,t}^\perp$ has parameters $\bar{\gamma} = 2r - t$ and $\bar{\delta} = t - r$. Now, the values of κ and $\bar{\kappa}$ are easily obtained by applying Proposition 2.1. ■

Let $v = (v_1, \dots, v_m)$ be an element in \mathbb{Z}_2^m or \mathbb{Z}_4^m . We denote by $\sigma(v)$ the right cyclic shift of v , i.e. $\sigma(v) = (v_m, v_1, \dots, v_{m-1})$. We recursively define $\sigma^j(v) = \sigma(\sigma^{j-1}(v))$, for $j = 2, 3, \dots$. For vectors $\mathbf{u} = (u \mid u') \in \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ we extend the definition of σ as the double right cyclic shift of \mathbf{u} , that is, $\sigma(\mathbf{u}) = (\sigma(u) \mid \sigma(u'))$.

A $\mathbb{Z}_2\mathbb{Z}_4$ -additive code $\mathcal{C} \subseteq \mathbb{Z}_2^\alpha \times \mathbb{Z}_4^\beta$ is a $\mathbb{Z}_2\mathbb{Z}_4$ -cyclic code if for each codeword $\mathbf{x} \in \mathcal{C}$, we have that $\sigma(\mathbf{x}) \in \mathcal{C}$. Such codes were first defined in [1] and also studied in [4]. As can be seen in [1], the dual of a $\mathbb{Z}_2\mathbb{Z}_4$ -cyclic code is also $\mathbb{Z}_2\mathbb{Z}_4$ -cyclic.

III. THERE IS NO NONTRIVIAL $\mathbb{Z}_2\mathbb{Z}_4$ -CYCLIC PERFECT CODES WITH ONE EXCEPTION

We say that a code is nontrivial if it has more than two codewords and its minimum distance is $d > 1$. Apart from 1-perfect codes, there is only another nontrivial binary perfect code. It is the linear binary Golay code of length 23. But this code has not any $\mathbb{Z}_2\mathbb{Z}_4$ -linear structure apart from the binary linear one [12]. Therefore, any binary nonlinear and nontrivial $\mathbb{Z}_2\mathbb{Z}_4$ -linear perfect code is a 1-perfect code.

In this section, we prove that for any $\mathbb{Z}_2\mathbb{Z}_4$ -linear 1-perfect code, which is not a Hamming code, its corresponding $\mathbb{Z}_2\mathbb{Z}_4$ -additive code cannot be $\mathbb{Z}_2\mathbb{Z}_4$ -cyclic with exactly one exception.

Proposition 3.1: If $\mathcal{C}_{r,t}$ is a $\mathbb{Z}_2\mathbb{Z}_4$ -cyclic 1-perfect code, then $t = r$ or $t = 2r$.

Proof: By the argument in the proof of Proposition 2.3, we may assume that $\mathcal{C}_{r,t}$ contains a codeword of the form $\mathbf{x} = (x \mid 2, 0, \dots, 0)$ with $w(x) = 1$. Now, consider the codeword $\mathbf{z} = \sigma^\beta(\mathbf{x})$. If $\mathbf{z} \neq \mathbf{x}$ then $\mathbf{z} + \mathbf{x}$ would have weight 2. Consequently, \mathbf{z} must be equal to \mathbf{x} implying that β is a multiple of α , that is, $2^{t-1} - 2^{r-1}$ is a multiple of $2^r - 1$. Thus,

$$\frac{2^{r-1}(2^{t-r} - 1)}{2^r - 1} \in \mathbb{N} \implies \frac{(2^{t-r} - 1)}{2^r - 1} \in \mathbb{N}.$$

Therefore r divides $t - r$ implying that r divides t . Since $r \leq t \leq 2r$, the only possibilities are $t = r$ or $t = 2r$. ■

If $t = r$, then $\mathcal{C}_{r,t} = \Phi(\mathcal{C}_{r,t})$ is linear, i.e. a Hamming code. In effect, it is well known that its coordinates can be arranged such that it is a binary cyclic code. We are interested in those codes whose binary Gray image is not linear, that is, when $t = 2r$. For this case, $t = 2r$, we have that $\mathcal{C}_{r,2r}$ is of type

$$(2^r - 1, 2^{r-1}(2^r - 1); 2^r - 1, 2^{r-1}(2^r - 1) - r; 2^r - 1),$$

and applying Proposition 2.3 we obtain that its dual code $\mathcal{C}_{r,2r}^\perp$ is of type

$$(2^r - 1, 2^{r-1}(2^r - 1); 0, r; 0).$$

Example 3.2: For $r = 2$ we have that the type of $\mathcal{C}_{2,4}$ is $(3, 6; 3, 4; 3)$. By Proposition 2.3, its dual code $\mathcal{C}_{2,4}^\perp$ is of type $(3, 6; 0, 2; 0)$. Consider the matrix

$$H = \left(\begin{array}{ccc|cccc} 1 & 1 & 0 & 1 & 1 & 2 & 3 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 2 & 3 & 1 \end{array} \right).$$

The matrix H generates a code of type $(3, 6; 0, 2; 0)$. Any column is not a multiple of another one. Hence the code \mathcal{C}^* with parity check matrix H has minimum distance at least 3, type $(3, 6; 3, 4; 3)$ and size 2^{11} . Therefore, \mathcal{C}^* is the $\mathbb{Z}_2\mathbb{Z}_4$ -additive 1-perfect code $\mathcal{C}_{2,4}$ and H generates $\mathcal{C}_{2,4}^\perp$. Note that the second row of H is the shift of the first one. Also, the first row minus the second one gives the shift of the second row. Since the shift of any row of H is a codeword, we have that the shift of any codeword is again a codeword. Consequently, $\mathcal{C}_{2,4}^\perp$ is a $\mathbb{Z}_2\mathbb{Z}_4$ -cyclic code and so is $\mathcal{C}_{2,4}$.

From now on, we denote by $D^{(r)}$ the code $\mathcal{C}_{r,2r}^\perp$ of binary length $n = \alpha + 2\beta = 2^{2r} - 1$. Hence, $D_b^{(r)}$ is the set of codewords of order 2 and the zero codeword. Recall that the dual of a binary Hamming code is called simplex.

Of course, the coordinates of a simplex code can be arranged such that the code is cyclic. We denote by S_r a cyclic simplex code of length $2^r - 1$.

Lemma 3.3: The code $D^{(r)}$ is a constant weight code, where all nonzero codewords have weight 2^{2r-1} .

Proof: The weight distributions of dual codes are related by the MacWilliams identity [7], [11], as well as for binary linear codes. It is well known that any 1-perfect code has the same weight distribution as the Hamming code of the same length. Therefore, $D^{(r)}$ must have the same weight distribution as the simplex code of length $n = 2^{2r} - 1$. Hence, the weight of any nonzero codeword is $(n + 1)/2 = 2^{2r-1}$. ■

Proposition 3.4: If $D^{(r)}$ is $\mathbb{Z}_2\mathbb{Z}_4$ -cyclic, then $(D^{(r)})_X = S_r$. Moreover, a codeword $\mathbf{z} \in D^{(r)}$ has the zero vector in the \mathbb{Z}_2 part, $\mathbf{z} = (0, \dots, 0 \mid z'_1, \dots, z'_\beta)$, if and only if $\mathbf{z} \in D_b^{(r)}$.

Proof: A generator matrix for $D^{(r)}$ would have the form

$$G = \left(G_1 \mid G_2 \right),$$

where G_1 is a $r \times 2^r - 1$ generator matrix for $(D^{(r)})_X$. Since the minimum weight of $\mathcal{C}_{r,2r}$ is 3, G_1 has neither repeated columns, nor the zero column. Therefore G_1 has as columns all the nonzero binary vectors of length r and $(D^{(r)})_X = S_r$. The size of $D^{(r)}$ is $|D^{(r)}| = 2^{2r}$ and the number of codewords of order less than or equal to 2 is $|D_b^{(r)}| = 2^r$. Hence, $D^{(r)}$ can be viewed as a set of 2^r cosets of $D_b^{(r)}$. We conclude that each codeword in $(D^{(r)})_X$ appears 2^r times in $D^{(r)}$. So, the zero codeword in $(D^{(r)})_X$ appears in $D^{(r)}$ exactly in the codewords of $D_b^{(r)}$. ■

Proposition 3.5: Suppose that $D^{(r)}$ is $\mathbb{Z}_2\mathbb{Z}_4$ -cyclic. If we change the coordinates '2' by '1' in $(D_b^{(r)})_Y$ we obtain 2^{r-1} copies of S_r .

Proof: Clearly, when we change the twos by ones in $(D_b^{(r)})_Y$, we obtain a binary linear cyclic code D with constant weight and dimension r . By [2], D must be a simplex code or a replication of a simplex code. Since the dimension is r , we conclude that D is a replication of a simplex code of length $2^r - 1$. Moreover, since $(D_b^{(r)})_Y$ is cyclic, D is a replication of S_r . ■

Therefore, if $D^{(r)}$ is $\mathbb{Z}_2\mathbb{Z}_4$ -cyclic, any order 4 codeword is of the form:

$$\mathbf{z} = (x_1, \dots, x_\alpha \mid y^{(1)}, \dots, y^{(2^{r-1})}),$$

where $y^{(i)} = (y_1^{(i)}, \dots, y_\alpha^{(i)})$, for all $i = 1, \dots, 2^{r-1}$. The set of coordinate positions of $y^{(i)}$ will be called the i th block. Taking into account that $2\mathbf{z} \in D_b^{(r)}$ and by Proposition 3.5, we see that \mathbf{z} has 2^{r-1} odd coordinates (i.e. coordinates from $\{1, 3\}$) in any block at the same positions. In other words, $y^{(i)} \equiv y^{(j)} \pmod{2}$, for all $i, j = 1, \dots, 2^{r-1}$.

Corollary 3.6: Let $\mathbf{z} = (x_1, \dots, x_\alpha \mid y^{(1)}, \dots, y^{(2^{r-1})}) \in D^{(r)}$ be an order 4 codeword and assume that $D^{(r)}$ is

$\mathbb{Z}_2\mathbb{Z}_4$ -cyclic. Then, $(y^{(1)}, \dots, y^{(2^{r-1})})$ has:

$$\begin{array}{ll} 2^{2r-2} & \text{odd coordinates} \\ 2^{r-2}(2^{r-1} - 1) & \text{twos, and} \\ 2^{r-2}(2^{r-1} - 1) & \text{zeroes.} \end{array}$$

Proof: The result follows from Lemma 3.3, Proposition 3.4 and Proposition 3.5. \blacksquare

For any binary vector $x = (x_1, \dots, x_m)$, the support of x is the set of nonzero positions, $\text{supp}(x) = \{i \mid x_i \neq 0\}$. Note that $w(x) = |\text{supp}(x)|$. We define $\overline{\text{supp}}(x) = \{1, \dots, m\} \setminus \text{supp}(x)$ as the complementary support of x .

Lemma 3.7: Let S_r be a cyclic simplex code of length $2^r - 1$, with $r > 2$. For any pair of codewords $x, y \in S_r$ we have that $|\text{supp}(x) \cap \overline{\text{supp}}(y)|$ is even. In other words, x cannot have an odd number of nonzero positions in $\overline{\text{supp}}(y)$.

Proof: The distance between x and y must be 2^{r-1} . Therefore,

$$d(x, y) = |\text{supp}(x)| + |\text{supp}(y)| - 2|\text{supp}(x) \cap \text{supp}(y)| = 2^{r-1}.$$

But the weight of any codeword is 2^{r-1} . Thus,

$$2^{r-1} + 2^{r-1} - 2|\text{supp}(x) \cap \text{supp}(y)| = 2^{r-1},$$

implying that $|\text{supp}(x) \cap \text{supp}(y)| = 2^{r-2}$, which is even for $r > 2$. Hence, $|\text{supp}(x) \cap \overline{\text{supp}}(y)|$ is also even for $r > 2$. \blacksquare

Proposition 3.8: Suppose that $D^{(r)}$ is $\mathbb{Z}_2\mathbb{Z}_4$ -cyclic and $r > 2$. Let $\mathbf{z} = (x_1, \dots, x_\alpha \mid y^{(1)}, \dots, y^{(2^{r-1})}) \in D^{(r)}$ be an order 4 codeword. For any distinct i, j , define

$$N_{i,j} = \{\ell \mid 1 \leq \ell \leq \alpha, y_\ell^{(i)}, y_\ell^{(j)} \in \{0, 2\}, y_\ell^{(i)} \neq y_\ell^{(j)}\},$$

i.e. $N_{i,j}$ is the set of coordinate positions where $y^{(i)}$ has a ‘2’ and $y^{(j)}$ has ‘0’ or vice versa. Then, $|N_{i,j}|$ is even.

Proof: Suppose to the contrary that $|N_{i,j}|$ is odd. Assume that $i < j$ and consider the codeword $\mathbf{v} = \sigma^{\alpha(j-i)}(\mathbf{z})$. Clearly, $\mathbf{u} = \mathbf{v} + \mathbf{z}$ has the zero vector in the \mathbb{Z}_2 part. Thus, by Proposition 3.4, \mathbf{u} is an order two codeword. Now, comparing with the codeword $2\mathbf{v}$ (or $2\mathbf{z}$), we can see that \mathbf{u} has an odd number of twos in $\overline{\text{supp}}(2\mathbf{v})$ in the j th block, contradicting Lemma 3.7. \blacksquare

As a consequence, we obtain that in any order 4 codeword, the number of twos in any block has the same parity.

Corollary 3.9: Suppose that $D^{(r)}$ is $\mathbb{Z}_2\mathbb{Z}_4$ -cyclic and $r > 2$. Let $(x_1, \dots, x_\alpha \mid y^{(1)}, \dots, y^{(2^{r-1})}) \in D^{(r)}$ be an order 4 codeword. Put $\eta_k(y) = |\{\ell \mid 1 \leq \ell \leq \alpha, y_\ell^{(k)} = 2\}|$. Then, $\eta_1(y), \dots, \eta_{2^{r-1}}(y)$ have all the same parity.

Proof: Straightforward from Proposition 3.8. \blacksquare

Lemma 3.10: Suppose that $D^{(r)}$ is $\mathbb{Z}_2\mathbb{Z}_4$ -cyclic and $r > 2$. As before, let $\mathbf{z} = (x_1, \dots, x_\alpha \mid y^{(1)}, \dots, y^{(2^{r-1})}) \in D^{(r)}$ be an order 4 codeword. Then, there exist different $k, k' \in \{1, \dots, 2^{r-1}\}$ such that $\eta_k(y) \neq \eta_{k'}(y)$. Moreover,

if for some $\ell \in \{1, \dots, \alpha\}$ we have $y_\ell^{(k)} = 0$ and $y_\ell^{(k')} = 2$, then

$$\begin{aligned} |\{i \mid 1 \leq i \leq 2^{r-1}, y_\ell^{(i)} = 0\}| &= \\ |\{j \mid 1 \leq j \leq 2^{r-1}, y_\ell^{(j)} = 2\}| &= 2^{r-2}. \end{aligned}$$

Proof: The total number of twos in \mathbf{z} is $2^{r-2}(2^{r-1} - 1)$ (see Corollary 3.6). But this number is not divisible by 2^{r-1} and hence not all the blocks have the same number of twos. This proves that $\eta_k(y) \neq \eta_{k'}(y)$ for some $k, k' \in \{1, \dots, 2^{r-1}\}$.

Let k and $k' = k + 1$ be such that $\eta_k(y) \neq \eta_{k'}(y)$. Without loss of generality, we assume that $k' = 2^{r-1}$ and $k = 2^{r-1} - 1$. After some shifts of \mathbf{z} , we can get the situation that $y_\alpha^{(k)} \neq y_\alpha^{(k')}$, where $y_\alpha^{(k)}, y_\alpha^{(k')} \in \{0, 2\}$. That is, the last coordinates of the last two blocks are in $\{0, 2\}$ and different from each other. Now, if we shift the codeword, $\eta_{2^{r-1}}(y)$ changes its parity. Hence, by Corollary 3.9, $\eta_{2^{r-1}-1}(y)$ must change its parity as well, implying that $y_\alpha^{(2^{r-1}-2)} \neq y_\alpha^{(2^{r-1}-1)}$ and $y_\alpha^{(2^{r-1}-2)}, y_\alpha^{(2^{r-1}-1)} \in \{0, 2\}$. With the same argument, $y_\alpha^{(2^{r-1}-3)} \neq y_\alpha^{(2^{r-1}-2)}$, $y_\alpha^{(2^{r-1}-3)}, y_\alpha^{(2^{r-1}-2)} \in \{0, 2\}$, and so on. Therefore, in this last coordinate, half of the blocks have a '0' and half of the blocks have a '2'. ■

Now, we are ready to prove the nonexistence of a $\mathbb{Z}_2\mathbb{Z}_4$ -cyclic code $D^{(r)}$ for $r > 2$.

Theorem 3.11: There is no $\mathbb{Z}_2\mathbb{Z}_4$ -cyclic 1-perfect code \mathcal{C} such that $C = \Phi(\mathcal{C})$ is nonlinear except for the case when $\mathcal{C} = \mathcal{C}^*$ is the code of Example 3.2 of type $(3, 6; 3, 4; 3)$, which is a $\mathbb{Z}_2\mathbb{Z}_4$ -cyclic code.

Proof: Assume that \mathcal{C} is a $\mathbb{Z}_2\mathbb{Z}_4$ -cyclic 1-perfect code such that $C = \Phi(\mathcal{C})$ is nonlinear. By Proposition 3.1, \mathcal{C} must be a code $\mathcal{C}_{r,2r}$. If $r = 2$, then we have seen the $\mathbb{Z}_2\mathbb{Z}_4$ -cyclic code $\mathcal{C}^* = \mathcal{C}_{2,4}$ in Example 3.2. Suppose now that $r > 2$.

Let $\mathbf{z} = (x_1, \dots, x_\alpha \mid y^{(1)}, \dots, y^{(2^{r-1})}) \in \mathcal{C}^\perp$ be an order 4 codeword. Define

$$\begin{aligned} \lambda &= \left| \left\{ \ell \mid 1 \leq \ell \leq \alpha, y_\ell^{(i)} = 2, \forall i = 1, \dots, 2^{r-1} \right\} \right|, \text{ and} \\ \mu &= \left| \left\{ \ell \mid 1 \leq \ell \leq \alpha, \text{ such that } \exists k, k' \text{ with } y_\ell^{(k)} \neq y_\ell^{(k')}; \right. \right. \\ &\quad \left. \left. y_\ell^{(k)}, y_\ell^{(k')} \in \{0, 2\} \right\} \right|. \end{aligned}$$

Then, by Lemma 3.10, the number of twos in \mathbf{z} is $2^{r-1}\lambda + 2^{r-2}\mu$. We have seen in Corollary 3.6 that this must equal $2^{r-2}(2^{r-1} - 1)$. Thus, we obtain

$$2\lambda + \mu = 2^{r-1} - 1,$$

implying that μ is an odd number. But this is a contradiction with Proposition 3.8. ■

IV. THE NONEXISTENCE OF NONTRIVIAL $\mathbb{Z}_2\mathbb{Z}_4$ -CYCLIC EXTENDED PERFECT CODES

Given a $\mathbb{Z}_2\mathbb{Z}_4$ -additive 1-perfect code $\mathcal{C}_{r,t}$ ($2 \leq r \leq t \leq 2r$), we denote by $\mathcal{C}'_{r,t}$ the extended code obtained by adding an even parity check coordinate (of course, at the \mathbb{Z}_2 part). Then, $\mathcal{C}'_{r,t}$ is a $\mathbb{Z}_2\mathbb{Z}_4$ -additive extended 1-perfect code. Recall that $\mathcal{C}_{r,t}$ is of type

$$(2^r - 1, 2^{t-1} - 2^{r-1}; 2^r - 1 - 2r + t, 2^{t-1} - 2^{r-1} + r - t; 2^r - 1 - 2r + t).$$

Since $|\mathcal{C}'_{r,t}| = |\mathcal{C}_{r,t}|$, $|(\mathcal{C}'_{r,t})_b| = |(\mathcal{C}_{r,t})_b|$, and $|((\mathcal{C}'_{r,t})_b)_X| = |((\mathcal{C}_{r,t})_b)_X|$, we have that $\mathcal{C}'_{r,t}$ is of type

$$(2^r, 2^{t-1} - 2^{r-1}; 2^r - 1 - 2r + t, 2^{t-1} - 2^{r-1} + r - t; 2^r - 1 - 2r + t).$$

In this section, we prove that $\mathcal{C}'_{r,t}$ is not $\mathbb{Z}_2\mathbb{Z}_4$ -cyclic for $t > 2$. For this, we begin examining the case $r = 2$. In such case, we have $t \in \{2, 3, 4\}$. The case $t = r = 2$ corresponds to a binary linear cyclic code of length 4 and two codewords. Such code is the trivial repetition code of length 4. Hence, we consider the cases $t = 3$ and $t = 4$.

Lemma 4.1: The codes $\mathcal{C}'_{2,3}$ and $\mathcal{C}'_{2,4}$ are not $\mathbb{Z}_2\mathbb{Z}_4$ -cyclic.

Proof: First, we consider the code $\mathcal{C}'_{2,3}$. The type of $\mathcal{C}'_{2,3}$ is $(4, 2; 2, 1; 2)$. Hence, $\mathcal{C}'_{2,3}$ contains 8 codewords of order 4. Let $\mathbf{x} = (x \mid x'_1, x'_2)$ be one such codeword. Since any codeword in $\mathcal{C}'_{2,3}$ has weight 4 or 8, it follows that x'_1 and x'_2 must be both odd coordinates (otherwise $2\mathbf{x}$ would have weight 2). Also, we have that $w(x) = 2$. If we consider the codeword $\mathbf{x} + \sigma(\mathbf{x})$, we can see that $x + \sigma(x)$ must have weight 4, implying that $x = (1, 0, 1, 0)$ (or $x = (0, 1, 0, 1)$). Now, take a codeword $\mathbf{y} = (y \mid y'_1, y'_2)$ such that $y'_1 = x'_1$ and $y'_2 \neq x'_2$ (a simple counting argument shows that exactly half of the codewords have equal the last two coordinates). We have that $d(x, y) \in \{0, 4\}$ and hence $d(\mathbf{x}, \mathbf{y}) \in \{2, 6\}$, a contradiction.

The code $\mathcal{C}'_{2,4}$ is an extension of the code \mathcal{C}^* in Example 3.2. Consider the dual code $\mathcal{D} = (\mathcal{C}'_{2,4})^\perp$. If H is a generator matrix for $\mathcal{C}_{2,4}^\perp$, then a generator matrix for \mathcal{D} can be obtained adding, first, a zero column to H and, second, the row $\mathbf{f} = (1, \dots, 1 \mid 2, \dots, 2)$. Hence, \mathcal{D} is of type $(4, 6; 1, 2; 1)$ and any nonzero codeword $\mathbf{z} \neq \mathbf{f}$ has weight 8. Let \mathbf{x} be an order 4 codeword. Clearly, \mathbf{x} must have 4 odd coordinates in the quaternary part (otherwise, $2\mathbf{x}$ would not have weight 8). This implies that $\mathbf{z} = \mathbf{x} + \sigma^4(\mathbf{x})$ is an order 4 vector. If \mathcal{D} is cyclic, then $\mathbf{z} = (z \mid z') \in \mathcal{D}$. Note that \mathbf{z} has zeros in all the binary positions, i.e. $z = (0, \dots, 0)$. Thus, z' has 4 odd coordinates and two coordinates, say z'_i and z'_j equal to '2'. But note that z'_i or z'_j (or both) is obtained as the addition of two odd coordinates. Therefore, $\mathbf{x} - \sigma^4(\mathbf{x})$ has weight less than 8, getting a contradiction. ■

Now, we establish the main result of this section.

Theorem 4.2: If $\mathcal{C}' = \mathcal{C}'_{r,t}$ is a $\mathbb{Z}_2\mathbb{Z}_4$ -additive extended 1-perfect code with $t \geq 3$, then \mathcal{C}' is not $\mathbb{Z}_2\mathbb{Z}_4$ -cyclic.

Proof: Consider the subcode $\mathcal{C}'_0 = \{(x \mid 0, \dots, 0)\}$. If \mathcal{C}' is $\mathbb{Z}_2\mathbb{Z}_4$ -cyclic, then clearly $(\mathcal{C}'_0)_X$ is a binary linear cyclic code. For every vector $\mathbf{v} = (v \mid 0, \dots, 0)$ of odd weight, we have that \mathbf{v} must be at distance 1 from one codeword in \mathcal{C}' . Since no codeword \mathbf{z} can have only an odd coordinate in the \mathbb{Z}_4 part (otherwise $2\mathbf{z}$ would have weight 2), it follows that v is at distance 1 from a codeword in $(\mathcal{C}'_0)_X$. Therefore \mathcal{C}'_0 must be an extended Hamming code. But such code cannot be cyclic unless it has length 4 [8]. The result then follows by Lemma 4.1. ■

REFERENCES

- [1] T. Abualrub, I. Siap and H. Aydin, “ $\mathbb{Z}_2\mathbb{Z}_4$ -additive cyclic codes,” *IEEE Trans. Inform. Theory*, vol. 60, pp. 1508-1514, 2014.
- [2] A. Bonisoli, “Every equidistant linear code is a sequence of dual Hamming codes,” *Ars Combin.*, vol. 18, pp. 181-186, 1984.
- [3] J. Borges, C. Fernández-Córdoba, J. Pujol, J. Rifà and M. Villanueva, “ $\mathbb{Z}_2\mathbb{Z}_4$ -linear codes: generator matrices and duality,” *Designs, Codes and Cryptography*, vol. 54, pp. 167-179, 2010.
- [4] J. Borges, C. Fernández-Córdoba and R. Ten-Valls, “ $\mathbb{Z}_2\mathbb{Z}_4$ -additive cyclic codes, generator polynomials and dual codes,” *arXiv: 1406.4425*, 2015.

- [5] J. Borges, K.T. Phelps and J. Rifà, “The rank and kernel of extended 1-perfect \mathbb{Z}_4 -linear and additive non- \mathbb{Z}_4 -linear codes,” *IEEE Trans. Inform. Theory*, vol. 49, pp. 2028-2034, 2003.
- [6] J. Borges and J. Rifà, “A characterization of 1-perfect additive codes,” *IEEE Trans. Inform. Theory*, vol. 45, pp. 1688-1697, 1999.
- [7] P. Delsarte and V. Levenshtein, “Association schemes and coding theory,” *IEEE Trans. Inform. Theory*, 44, pp. 2477-2504 (1998).
- [8] J. Justensen and S. Forchhammer, *Two-dimensional Information Theory and coding*, Cambridge Univ. Press., 2010.
- [9] D.S. Krotov, “ \mathbb{Z}_4 -linear perfect codes”, *Diskret. Anal. Issled. Oper.*, Ser. 1. 7(4), pp. 78–90, 2000. In Russian.
- [10] F.J. MacWilliams and N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Publishing Company, 1977.
- [11] J. Pujol and J. Rifà, “Translation-invariant propelinear codes,” *IEEE Trans. Inform. Theory*, vol. 43, pp. 590-598, 1997.
- [12] J. Rifà, “On a categorial isomorphism between a class of completely regular codes and a class of distance regular graphs. *Applied Algebra, Algebraic Algorithms and Error-Correcting Codes*, AAECC-8, vol. 508 LNCS, pp. 164-179, 1990.